

a

WHAT IS CLAIMED IS:

Patent Claims,

1. A method for the simplified implementation of encryption methods, particularly the Vernam cipher, where the encryption process may be a very simple mathematical operation, such as EXOR, characterized in that

- with the aid of a secret key (KS) having a defined key length (x bits) and using an optionally variable parameter (IV) having a length of $n \cdot x$ bits, a Vernam key (KV) having the length of the message to be encrypted is generated by way of any symmetrical cipher (S);
- using logic operations of the Vernam cipher (V), the Vernam key (KV) encrypts the message to be protected;
- the secret key (KS) and the parameter (IV) are communicated from the sender to the recipient via a secure channel separate from the message-transmission path or directly on the message-transmission path, secured by an asymmetrical method (A) or the like; and
- the recipient regenerates the Vernam key (KV) and therewith decrypts the received message.

2. The method as recited in claim 1, characterized in that

- the symmetrical cipher and the storage for the Vernam key (KV) are installed in a crypto-module, separate from the encryptor, in the form of a

chipcard, a multifunctional PC interface adapter or module (PCMCIA); and

- only the Vernam cipher operations are performed in the encryptor.

3. The method as recited in claim 1, characterized in that

the asymmetrical cipher and the storage for the Vernam key (KV) are implemented in an external crypto-module separate from the encryptor; and

- the Vernam cipher controls the encryption operations in the encryptor.

4. The method as recited in one of claims 1 through 3, characterized in that the Vernam key (KV) is stored in the encryptor.

5. A device for implementing the methods as recited in one of claims 1 through 4, characterized in that

- the crypto-hardware is composed of a chipcard or a multifunctional PC interface adapter (PCMCIA module) or the like, with built-in special crypto-hardware; and
- the encryptor is made of a conventional personal computer or the like, software or another terminal which implements a very simple Vernam cipher for broad-band applications in software

6. The device according to one of the methods as recited in claims 1 through 4, characterized in that the crypto-

013
am4

hardware is designed as an external crypto-module and has an intermediate storage for the reserve storage of the Vernam key (KV).

7. The device as recited in one of claims 6 and 7, characterized in that the storage for storing the Vernam key (KV) is disposed either in the personal computer (PC) or in another terminal.

SECRET